

Rec'd PCT/STO

08 MAR 2005

PCT/JP 03/16437

22.12.03

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

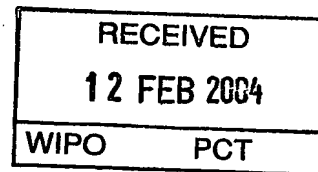
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2002年12月26日

出 願 番 号  
Application Number: 特願2002-378555  
[ST. 10/C]: [JP2002-378555]

出 願 人  
Applicant(s): 松下電器産業株式会社

Best Available Copy

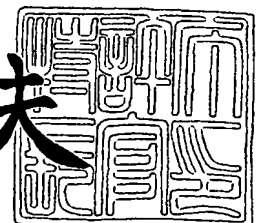


**PRIORITY DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 1月30日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特2004-3004370

【書類名】 特許願  
【整理番号】 2037340040  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 13/00  
H04L 12/00  
H04L 29/10

## 【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 渡邊 崇弘

## 【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 ▲はま▼木 貴之

## 【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

## 【代理人】

【識別番号】 100109210

## 【弁理士】

【氏名又は名称】 新居 広守

## 【手数料の表示】

【予納台帳番号】 049515

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0213583

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワーク装置、通信過負荷回避方法およびプログラム

【特許請求の範囲】

【請求項 1】 ネットワークを介して通信する通信手段と、  
通信が過負荷状態にあるか否かを判定する判定手段と、  
判定結果による過負荷状態であると判定されたとき前記通信手段により受信されたデータを無効にする無効化手段と  
を備えることを特徴とするネットワーク装置。

【請求項 2】 前記判定手段は、ネットワークからの単位時間当たりの受信データの量がしきい値を超えたとき過負荷状態にあると判定することを特徴とする請求項 1 記載のネットワーク装置。

【請求項 3】 前記判定手段は、データリンク層に相当する通信処理における受信データについて前記しきい値による判定を行うことを特徴とする請求項 2 記載のネットワーク装置。

【請求項 4】 ネットワーク装置は、さらに、ネットワーク装置における通信以外の処理負荷の状態に応じて、動的に前記しきい値を決定する決定手段を備え、

前記判定手段は、決定されたしきい値により過負荷状態であるか否かを判定することを特徴とする請求項 2 又は 3 記載のネットワーク装置。

【請求項 5】 前記決定手段は、ネットワーク装置が実行中のアプリケーションプログラムの数に応じてしきい値を決定することを特徴とする請求項 4 記載のネットワーク装置。

【請求項 6】 前記通信手段は、  
物理層及びデータリンク層に相当する通信処理を行う第 1 通信処理部と、  
第 1 通信処理部からの受信データを一時的に保持するメモリと、  
メモリに保持された受信データを取り出してネットワーク層以上の層に相当する通信処理を行う第 2 通信処理部と  
を有し、

前記判定手段は、前記メモリに保持された受信データの量がしきい値を超えた

ときに、過負荷状態であると判定する

ことを特徴とする請求項 1 記載のネットワーク装置。

【請求項 7】 前記通信手段は、階層的な通信処理を行い、  
前記無効化手段は、何れかの階層間の論理的な接続を禁止する  
ことを特徴とする請求項 1 乃至 6 の何れか 1 項に記載のネットワーク装置。

【請求項 8】 前記通信手段は、  
物理層及びデータリンク層に相当する通信処理を行う第 1 通信処理部と、  
ネットワーク層以上に相当する第 2 通信処理部と  
を有し、  
前記無効化手段は、前記第 1 通信処理部から第 2 通信処理部への受信データの  
通知を禁止する

ことを特徴とする請求項 1 乃至 6 の何れか 1 項に記載のネットワーク装置。

【請求項 9】 ネットワークを介して通信する通信手段と、  
通信が過負荷状態になったことを検出する第 1 検出手段と、  
過負荷状態になったことが検出されたとき前記通信手段により受信されたデー  
タを無効にする無効化手段と  
過負荷状態が解消されたことを検出する第 2 検出手段と、  
過負荷状態が解消されたことが検出されたとき無効化手段による無効化を解除  
する解除手段と  
を備えることを特徴とするネットワーク装置。

【請求項 10】 前記第 1 検出手段は、ネットワークからの単位時間当たり  
の受信データの量が第 1 のしきい値を超えたとき過負荷状態になったと検出し、  
前記第 2 検出手段は、第 1 検出手段により過負荷状態になったことが検出され  
た後、前記通信手段に受信される単位時間当たりのデータの量が第 2 のしきい値  
を下回ったかを調査することにより過負荷状態が解消されたことを検出する  
ことを特徴とする請求項 9 記載のネットワーク装置。

【請求項 11】 前記通信手段は、階層的な通信処理を行い、  
前記無効化手段は、何れかの階層間の論理的な接続を禁止する  
ことを特徴とする請求項 10 に記載のネットワーク装置。

【請求項 1 2】 前記通信手段は、  
物理層及びデータリンク層に相当する通信処理を行う第 1 通信処理部と、  
ネットワーク層以上に相当する第 2 通信処理部と  
を有し、  
前記第 1 検出手段は、第 1 通信処理部に受信されたデータについて第 1 のしき  
い値による判定を行い、  
前記無効化手段は、前記第 1 通信処理部から第 2 通信処理部への受信データの  
通知を禁止し、  
前記第 2 検出手段は、第 1 通信処理部に受信されるデータの量が第 2 のしき  
い値を下回ったかを調査する  
ことを特徴とする請求項 1 1 記載のネットワーク装置。

【請求項 1 3】 前記第 1 通信部は、割り込み信号により第 2 通信処理部に  
受信データを通知し、  
前記無効化手段は、前記割り込み信号をマスクすることによって前記通知を禁  
止し、  
前記解除手段は、前記割り込み信号のマスクを解除する  
ことを特徴とする請求項 1 2 記載のネットワーク装置。

【請求項 1 4】 ネットワークを介して通信する通信部を有するネットワー  
ク装置における通信過負荷回避方法であって、  
通信が過負荷状態にあるか否かを判定する判定ステップと、  
判定結果による過負荷状態であると判定されたとき前記通信部により受信され  
たデータを無効にする無効化ステップと  
を有することを特徴とする通信過負荷回避方法。

【請求項 1 5】 前記判定ステップにおいて、ネットワークからの単位時間  
当たりの受信データの量がしきい値を超えたとき過負荷状態にあると判定する  
ことを特徴とする請求項 1 4 記載の通信過負荷回避方法。

【請求項 1 6】 前記判定ステップにおいて、データリンク層に相当する通  
信処理における受信データについて前記しきい値による判定を行う  
ことを特徴とする請求項 1 5 記載の通信過負荷回避方法。

【請求項 17】 通信過負荷回避方法は、さらに、ネットワーク装置における通信以外の処理負荷の状態に応じて、動的に前記しきい値を決定する決定ステップを有し

前記判定ステップにおいて、決定されたしきい値により過負荷状態であるか否かを判定する

ことを特徴とする請求項 15 又は 16 記載の通信過負荷回避方法。

【請求項 18】 前記決定ステップにおいて、ネットワーク装置が実行中のアプリケーションプログラムの数に応じてしきい値を決定する

ことを特徴とする請求項 18 記載の通信過負荷回避方法。

【請求項 19】 前記通信部は、物理層及びデータリンク層に相当する通信処理を行う第 1 通信処理部と、第 1 通信処理部からの受信データを一時的に保持するメモリと、メモリに保持された受信データを取り出してネットワーク層以上の層に相当する通信処理を行う第 2 通信処理部とを有し、

前記判定ステップにおいて、前記メモリに保持された受信データの量がしきい値を超えたときに、過負荷状態であると判定する

ことを特徴とする請求項 14 記載の通信過負荷回避方法。

【請求項 20】 前記通信部は、階層的な通信処理を行い、前記無効化ステップは、何れかの階層間の論理的な接続を禁止することを特徴とする請求項 14 乃至 19 の何れか 1 項に記載の通信過負荷回避方法。

【請求項 21】 前記通信部は、物理層及びデータリンク層に相当する通信処理を行う第 1 通信処理部と、ネットワーク層以上に相当する第 2 通信処理部とを有し、

前記無効化ステップは、前記第 1 通信処理部から第 2 通信処理部への受信データの通知を禁止する

ことを特徴とする請求項 14 乃至 19 の何れか 1 項に記載の通信過負荷回避方法。

【請求項 22】 請求項 14 乃至 21 の何れか 1 項に記載の通信過負荷回避

方法をコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明では、通信の過負荷状態に起因する悪影響を排除するネットワーク装置に関し、特に家庭内で映像データを取り扱うネットワーク装置に関する。

【0002】

【従来の技術】

一般に、IPネットワーク網に接続されたネットワーク装置において通信が過負荷な状態に陥ると、ネットワーク装置におけるIPレイヤー以下の通信処理の負荷が重くなり、CPUの処理能力が通信処理により大きく占有されるため、通信処理だけでなくその他の処理にも悪影響を及ぼす。

【0003】

また、通信が過負荷な状態に陥る端的な一例としてDoS攻撃 (Denial of Service attack) を受けた場合が考えられる。DoS攻撃により通信の過負荷状態に陥るのを回避する技術として、特許文献1記載の不正アクセス防御システムがある。このシステムでは、図8に示す構成において、攻撃検出機器2によりDoS攻撃を受けていることを検出した場合に、ネットワーク管理者の判断に従って、通信制御機器3は攻撃元のネットワークに通信制御の指示を通知して、攻撃元のルータ (攻撃遮断機器100、200) にてIP (Internet Protocol) パケットをフィルタリングするよう構成されている。このような構成により、通信過負荷状態を回避している。

【0004】

【特許文献1】

特開 2002-158660

【0005】

【発明が解決しようとする課題】

しかしながら、上記従来技術によれば、専門的な知識を有するネットワーク管理者の判断を必要とする点と、攻撃元のネットワークにフィルター機能を有する



装置を付加する必要がある点とで、一般家庭で使用されるネットワーク機器に適用することは困難である。

#### 【0006】

また、映像データを処理するネットワーク機器では、通信処理の過負荷によって通信処理にCPUが占有されてしまい、通信処理以外の主要な処理（映像データの処理等）を遅延させる悪影響を及ぼすと、ユーザに故障と誤解される可能性がある。特に、映像データ処理はリアルタイム性を要求されるので、通信過負荷状態に起因する影響を完全に排除する必要がある。

#### 【0007】

そこで本発明は、ユーザ判断及び外部の付加装置を必要としないで装置単体で通信過負荷状態を回避して、本体の処理を円滑にするネットワーク装置を提供することを目的とする。

#### 【0008】

##### 【課題を解決するための手段】

上記目的を達成するため本発明のネットワーク装置は、ネットワークを介して通信する通信手段と、通信が過負荷状態にあるか否かを判定する判定手段と、判定結果による過負荷状態であると判定されたとき前記通信手段により受信されたデータを無効にする無効化手段とを備える。

#### 【0009】

この構成によれば、過負荷状態では受信されたデータを無効化するので、ユーザによる判断も付加装置も必要としないで、通信の過負荷状態でも通信処理及び他の処理への影響を除去することができる。つまり、受信処理がCPUの処理能力を占有しないので、その他の処理の品質を落とすことなく継続することが可能となる。それゆえ、一般家庭で使用されるネットワーク装置でも容易に適用でき、他の処理を円滑にすることができる。例えば、通信処理以外の他の処理として、リアルタイム性を要求される映像データの処理を行うネットワーク装置であっても通信過負荷状態に起因する影響を排除することができる。

#### 【0010】

ここで、前記判定手段は、ネットワークからの単位時間当たりの受信データの

量がしきい値を超えたとき過負荷状態にあると判定する構成としてもよい。

この構成によれば、受信データ量に対するしきい値判断によって過負荷状態になったことを即時に判定することができる。

#### 【0011】

また、前記判定手段は、データリンク層に相当する通信処理における受信データについて前記しきい値による判定を行う構成としてもよい。

この構成によれば、しきい値判断をデータリンク層のレベルで行うので、ネットワーク層以上にしきい値判断の負荷がかからない。

#### 【0012】

さらに、前記ネットワーク装置は、ネットワーク装置における通信以外の処理負荷の状態に応じて、動的に前記しきい値を決定する決定手段を備え、前記判定手段は、決定されたしきい値により過負荷状態であるか否かを判定する構成としてもよい。

#### 【0013】

この構成によれば、しきい値を動的に決定するので、ネットワーク装置における通信処理以外の処理の負荷が大きいときと小さいときとで、通信過負荷状態を動的に変更することができる。その結果、ネットワーク装置における通信処理以外のリアルタイム性を要する処理などへの影響を除去し、しかも、ネットワーク装置全体の処理能力を最大限に発揮させることができる。

#### 【0014】

また、前記決定手段は、ネットワーク装置が実行中のアプリケーションプログラムの数に応じてしきい値を決定する構成としてもよい。

この構成によれば、しきい値の決定を動的に、実行中のアプリケーションプログラムの数に応じて簡単に行うことができる。

#### 【0015】

前記通信手段は、物理層及びデータリンク層に相当する通信処理を行う第1通信処理部と、第1通信処理部からの受信データを一時的に保持するメモリと、メモリに保持された受信データを取り出してネットワーク層以上の層に相当する通信処理を行う第2通信処理部とを有し、前記判定手段は、前記メモリに保持され

た受信データの量がしきい値を超えたときに、過負荷状態であると判定する構成としてもよい。

#### 【0016】

この構成によれば、第2通信処理部における通信処理（例えばIPプロトコル処理）において過負荷状態検出する。

また、前記通信手段は、階層的な通信処理を行い、前記無効化手段は、何れかの階層間の論理的な接続を禁止する構成としてもよい。

#### 【0017】

この構成によれば、接続を禁止された層以上の通信処理層に負荷がかからないことに加えて、通信処理以外のネットワーク装置の処理に処理負荷がかからない。これにより、通信過負荷状態においても、通信処理以外の処理は影響を受けることない。

#### 【0018】

さらに、前記無効化手段は、前記第1通信処理部から第2通信処理部への受信データの通知を禁止する構成としてもよい。

この構成によれば、無効化手段は、受信データの通知を禁止するだけで、通信過負荷状態においてネットワーク層以上の層の通信処理の負荷を除去することができる。第2通信処理部の処理がソフトウェアとCPUとにより実現されている場合には、CPUへの通信処理負荷を除去することができる。

#### 【0019】

また、本発明のネットワーク装置は、ネットワークを介して通信する通信手段と、通信が過負荷状態になったことを検出する第1検出手段と、過負荷状態になったことが検出されたとき前記通信手段により受信されたデータを無効にする無効化手段と、過負荷状態が解消されたことを検出する第2検出手段と、過負荷状態が解消されたことが検出されたとき無効化手段による無効化を解除する解除手段とを備える構成としてもよい。

#### 【0020】

また、本発明の通信過負荷状態回避方法、およびそのプログラムは、上記ネットワーク装置と同様の手段を有し、上記と同様の作用及び効果を奏する。

## 【0021】

## 【発明の実施の形態】

## ＜通信過負荷状態回避装置のハードウェア構成＞

図1は、本発明の実施の形態におけるネットワーク装置の主要なハードウェア構成を示す図である。このネットワーク装置は、同図では、通信過負荷状態回避装置10と称し、CPU (Central Processing Unit) 11、メモリ12、割り込みコントローラ13、LANチップ14、LAN I/F (interface) 15を備え、IP (Internet Protocol) ネットワーク17を介して通信ホスト16等と通信する。

## 【0022】

このハードウェア構成は一般的な構成であるが、メモリ12には本発明の通信過負荷状態回避方法を記述したプログラムが格納されている。このプログラムをCPU11が実行することによって、通信過負荷状態回避装置10は通信過負荷状態にあるか否かを判定し、過負荷状態であると判定されたとき、受信されたデータを無効にするように構成されている。ここで通信の過負荷状態とは、通信過負荷状態回避装置10における通信以外の他の処理（例えばリアルタイム性を要する映像データの処理）が正常に実行されなくなる状態をいう。

## 【0023】

まず、通信過負荷でない状態（以下、定常状態と呼ぶ。）におけるデータ受信時のハードウェア上の動作について説明する。

LANチップ14は、例えば、IEEE (Institute of Electrical and Electronic Engineers) 802.3規格（イーサネット（R）と呼ばれる）に準拠する物理層の一部及びデータリンク層の通信処理を行うコントローラであって、LAN I/F 15を介して自身のアドレス宛てのフレーム（イーサネット（R）フレームと呼ばれる）を受信すると、割り込みコントローラ13にその旨を通知する。この通知を受けた割り込みコントローラ13は、さらにCPU11に受信割り込みを発生する。この受信割り込みは、受信データが到着していることを通知する割り込みである。

## 【0024】

受信割り込みを受けると、CPU11は、LANチップ14が受信したデータをLANチップ14内のバッファから読み出してメモリ12へ転送し、IPプロトコル処理を行う。その際、定常状態では、CPU11はメモリ12内のプログラムを実行することによって、単位時間あたりのデータ受信量を調査することによって通信過負荷状態を検出する処理を行っている。

#### 【0025】

次に、通信過負荷状態（以下、異常状態とも呼ぶ。）を検出し、回避し、復旧するときのハードウェア上の動作について説明する。

通信ホスト16がネットワーク装置10に対して大量の通信を開始したものとする。CPU11は、通信が過負荷な状態であることを検出すると、割込みコントローラ13に対して、LANチップ14からの割込み信号をマスクする。これにより、CPU11ではEthernet（R）の受信割込みが発生しなくなり、通信過負荷状態を回避している。

#### 【0026】

異常状態では、CPU11はメモリ12内のプログラムを実行することによって、過負荷状態の終了を検出する処理を行い、過負荷状態の終了を検出すると割込みコントローラ13に対して上記の割込みマスクを解除する。これにより異常状態から定常状態に復旧する。以上が、ハードウェアからみた動作の概要である。

#### 【0027】

##### <通信過負荷状態回避装置の機能的な構成>

図2は、図1に示した通信過負荷状態回避装置10の主要な構成を機能別に表したブロック図である。同図の通信過負荷状態回避装置10は、LANチップ14、LANI/F15、ネットワークドライバ23、IPプロトコル処理部24、過負荷状態検出部25および過負荷状態終了検出部26を備える。図1と同じ構成要素には同じ番号を付与している。

#### 【0028】

LANチップ14は、OSI（Open System Interconnection）参照モデルにおける物理層の一部に相当するPHY層21における通信処理と、データリンク

層の一部に相当するMAC層22における通信処理とを行う。

#### 【0029】

LANI/F15は、物理層の一部に相当する処理として、LANチップ14とIPネットワークとの間で送受信すべきフレームをLANチップ14の電氣的仕様に適合させる。

#### 【0030】

ネットワークドライバ23は、定常状態において、データリンク層の一部に相当する通信処理を行う。この通信処理は、通常のいわゆるデバイスドライバとしての処理であり、図1において既に説明した受信割り込みに応じて行うLANチップ14からメモリ12へのデータ転送を含む。異常状態では割り込み信号がマスクされるので、ネットワークドライバ23は実質的に処理が禁止されることになる。

#### 【0031】

IPプロトコル処理部24は、定常状態において、ネットワークドライバ23から送受信されるデータに対してIPプロトコル処理を行う。

過負荷状態検出部25は、定常状態において、単位時間当たりの受信データ量がしきい値を超えていれば通信過負荷状態であると判定し、割り込みコントローラ13からCPU11への割り込み信号をマスクする。

#### 【0032】

過負荷状態終了検出部26は、異常状態において、LANチップ14内のバッファに受信されたフレームがあるか否かをチェックするポーリング処理を行い、受信されたフレームが存在しない状態が一定期間継続すれば過負荷状態終了と判断し、割り込みコントローラ13に対して上記の割り込みマスクを解除する。

#### 【0033】

なお、上記、過負荷状態検出部25は、単位時間当たりの受信データ量がしきい値を超えたか否かを判断する具体的な方法として、一定時間（例えば10ms）の受信データ量（例えば、ビット数、バイト数、フレーム数、IPパケット数等で表される量）を測定し、その測定結果に対してしきい値判定を行ってもよいし、一定量（例えば、ビット数、バイト数、フレーム数、IPパケット数の何れ

かで表される量)の受信データが到達した時間を測定し、その測定結果に対してしきい値判定を行ってもよい。

#### 【0034】

##### <通信過負荷状態検出処理の詳細フロー>

過負荷状態検出部25が、単位時間当たりの受信データ量がしきい値を超えたか否かを判断する具体例として、一定量(フレーム数でW個)の受信データが到達した時間を測定し、その測定結果に対してしきい値判定を行う例を説明する。

#### 【0035】

図3は、過負荷状態検出部25における通信過負荷状態検出処理の詳細例を示すフローチャートである。ただし、図中のS300~S302、S309は過負荷状態検出部25によってなされる通信過負荷状態検出処理の一部ではない。S300~S302は図1における受信割り込みにより通信過負荷状態検出処理が起動されるまでの処理を示し、S309はネットワークドライバ23の通信処理を示している。

#### 【0036】

また、図中のフレームカウンタは、W個のフレームをカウントするためのカウンタであり、Wから0までダウンカウントされる。タイムスタンプ $T_n$ は、通信過負荷状態回避装置10内のリアルタイムクロックから得られる時刻を保持するレジスタであり、現在のフレームを受信した時刻を示す。タイムスタンプ $T_{n-1}$ は現在のフレームよりもW個前に受信したフレームを受信した時刻を保持するためのレジスタである。 $T_n - T_{n-1}$ は、W個のフレームを受信した時間間隔を意味する。しきい値Aは、時間間隔( $T_n - T_{n-1}$ )が、短すぎる(過負荷状態)か否かを判定するためのしきい値である。しきい値Aは、通信処理によって通信過負荷状態回避装置10の他の処理に悪影響を及ぼさないように設定される。また、フレームカウンタ、タイムスタンプ $T_n$ 、 $T_{n-1}$ は何れも初期値を0とする。

#### 【0037】

定常状態においてLANチップ14は、LANI/F15を介してフレームを受信する(S300)と、割り込みコントローラ13を通して受信割り込みを発生

(S301) する。これを受けたCPU11は、過負荷状態検出部25に対応するプログラムを呼び出すことにより過負荷状態検出部25を起動する(S302)。

#### 【0038】

これ後の処理について、初回のフレーム受信時と2回目以降とに分けて説明する。

初回のフレーム受信では、過負荷状態検出部25は、フレームカウンタが0なので(S306)、タイムスタンプ $T_n$ の値を $T_{n-1}$ に代入し(S305)、タイムスタンプ $T_n$ の値としてリアルタイムクロックから現在時刻を取得し(S306)、フレームカウンタにスタート値 $W$ を設定する(S307)。これにより、2回目以降の受信の準備として、タイムスタンプ $T_n$ が現在のフレーム受信時刻に、フレームカウンタの値が $W$ に更新される。 $T_{n-1}$ は0のままである。更に、過負荷状態検出部25は、 $(T_n - T_{n-1})$ がしきい値 $A$ よりも大きいので(S308)、ネットワークドライバ23を起動して受信処理を行わせる(S309)。

#### 【0039】

二回目以降のフレーム受信では、過負荷状態検出部25は、フレームカウンタが0でなければ、つまり $W$ 個のフレームを受信していなければ(S303:偽)、フレームカウンタをデクリメントし(S304)、ネットワークドライバ23を起動して受信処理を行わせる(S309)。

#### 【0040】

また、フレームカウンタが0であれば、つまり $W$ 個のフレームを受信していれば(S303:真)、タイムスタンプ $T_n$ の値を $T_{n-1}$ に代入する(S305)。これにより、タイムスタンプ $T_{n-1}$ は、 $W$ 個前のフレームの受信時刻を示す。さらに、過負荷状態検出部25は、リアルタイムクロックから現在時刻を取得し、現在のフレームの受信時刻としてタイムスタンプ $T_n$ の値に設定し(S306)、時間間隔 $(T_n - T_{n-1})$ がしきい値 $A$ よりも小さい場合は(S307:真)、割り込みコントローラ13の割り込み信号をマスクし(S310)、通信の過負荷状態を検出したことを示す通知を11に発行し(S311)、過負荷状態終了



検出部 26 を起動する (S312)。

#### 【0041】

この割り込みマスクによって、割り込みコントローラ 13 から CPU 11 への割り込みが通知されなくなる。以後、LAN の通信に関するハードウェア割り込み処理が発生しなくなり、ネットワークドライバ 23 及び過負荷状態検出部 25 は起動されなくなる。その代わりに通信過負荷状態終了検出処理タスクが実行される。

#### 【0042】

一方、時間間隔 ( $T_n - T_{n-1}$ ) がしきい値 A よりも小さい場合は (S307: 偽)、過負荷状態ではないので、ネットワークドライバ 23 を起動して受信処理を行わせる (S309)。

#### 【0043】

<しきい値の例>

上記のしきい値 A は、CPU 11 の処理能力にも依存するが、例えば LAN の伝送速度が 100 Mbps の場合は、(フレームカウンタのスタート値 W、しきい値 A) を (85 個、10 mS) や (170 個、20 mS) とすればよい。また、10 Mbps の場合は、(8 個、10 mS) や (17 個、20 mS) とすればよい。しきい値 A には、通常発生するバースト性のフレーム受信の最大時間よりも十分に長い時間とするべきである。

#### 【0044】

また、上記しきい値 A の値は、通信過負荷状態回避装置 10 における通信以外の処理負荷の状態に応じて動的に決定することができる。その場合、図 3 に示した S307 と S308 の間に、しきい値を決定するステップを設ける構成とすればよい。このしきい値決定ステップにおいて、過負荷状態検出部 25 は、例えば図 5 に示すように、CPU 11 が実行中のアプリケーション数 L に応じて予め複数のしきい値 A1、A2・・・を対応させておき、現在実行中のアプリケーションの数に対応するしきい値を判定用のしきい値 A として決定する。

#### 【0045】

このようにしきい値を動的に決定することにより、通信過負荷状態回避装置 1

0における通信処理以外の処理の負荷が大きいときと小さいときとで、CPU 11の処理能力のうち通信処理が占有してよい部分を動的に変更することができ、通信過負荷状態を動的に定義することができる。その結果、通信過負荷状態回避装置10における通信処理以外のリアルタイム性を要する処理などへの影響を除去し、しかも、通信過負荷状態回避装置10全体の処理能力を最大限に発揮させることができる。

#### 【0046】

さらに、上記しきい値決定ステップでは、実行中のアプリケーションの数に対応させてしきい値を決定しているが、アプリケーションに重み付けをしてもよい。すなわち、過負荷状態検出部25は、処理量の多いアプリケーションや、リアルタイム性を要するアプリケーションについては、アプリケーション数を1ではなく2、3など重み付けた数に換算して全体のアプリケーション数を求めて、対応するしきい値を決定する。図6に、アプリケーション毎の重み付けた換算値を示す。同図では、アプリケーションApp1、4、5等は1のままであるが、App2は、そのアプリケーション数を2と換算し、同様にアプリケーションApp3は3と換算することを示している。

これによりアプリケーション毎に異なる処理量の差を吸収することができ、より適切なしきい値を動的に決定することができる。

#### 【0047】

##### <過負荷状態終了検出処理の詳細例>

過負荷状態検出部25によって過負荷状態が検出されると、過負荷状態終了検出部26が起動され過負荷状態の終了を検出する処理を行う。

#### 【0048】

図4は、過負荷状態終了検出部26における過負荷状態の終了を検出する処理の詳細例を示すフローチャートである。同図において、ループ1は一定時間（例えば10mS）の間連続して繰り返し実行されるループ処理であり、ループ2は一定期間（例えば5秒）毎に一回実行されるループ処理である。つまり、過負荷状態終了検出部26は、ポーリング処理として5秒毎に10mSのループ1の処理を行っている。また、Nは、通信過負荷状態が解消された可能性が高いと判定

された回数を意味し、0～5までをカウントするアップカウンタの値である。

#### 【0049】

まず、過負荷状態終了検出部26は、カウンタの値を $N=0$ に初期化し(S400)する。さらに、ループ1の処理として、LANチップ14のバッファ内に受信データが保持されているかどうかをチェックし(S403)、受信データが保持されていれば、当該受信データを読み出して(S404)、受信データから構成されるフレームの数 $m$ をカウントする(S405)。この繰り返しがループ1として10mSの間継続して実行される。その結果10mSの間に受信フレーム数 $m$ がカウントされる。

#### 【0050】

ループ1終了後に、過負荷状態終了検出部26は、受信フレーム数 $m$ がしきい値 $B$ より小さいか否かを判別し(S407)、小さければ $N$ をインクリメント( $N=N+1$ )し(S408)、大きければ $N$ をクリア( $N=0$ )する(S409)。受信フレーム数 $m$ がしきい値 $B$ よりも小さい場合は、通信の過負荷状態が解消している可能性が高いことを意味する。ここで、しきい値 $B$ は、例えば、伝送速度が100Mbpsの場合は85、10Mbpsの場合は8でよく、上記しきい値 $A$ と同じ値としてもよいし、図4、5に示したようにしきい値 $A$ と同様に動的に決定してもよい。

#### 【0051】

さらに、過負荷状態終了検出部26は、 $N$ が5以上か否かを判定する(S410)。この判定では、過負荷状態が解消している可能性が高いというループ1の結果が連続して5回あった場合に、通信過負荷状態終了と判定している。

#### 【0052】

$N$ が5より小さいと判定された場合には、過負荷状態検出部25は5秒後に再度ループ2の1回分の処理を実行する。 $N$ が5以上と判定された場合には、割り込みコントローラ13に対して割り込みマスクを解除し(S412)、過負荷状態が終了したことをCPU11に通知し(S413)、本処理を終える。

これにより、割り込みマスクが解除され異常状態から定常状態に戻る。

#### 【0053】

### <システム例>

以下、図1、2に示したネットワーク装置（通信過負荷状態回避装置10）を家電製品に適用した場合の実施例について説明する。

#### 【0054】

図7は、通信過負荷状態回避装置10を適用した家電製品を含むシステム例を示す図である。同図のシステムでは、STB（セットトップボックス）10a、DVDレコーダ10b、ホームサーバ10c、パソコン103及びネットワークI/F104がLANに接続され、さらにネットワークI/F104を介してインターネット上の配信サーバ105に接続されている。

#### 【0055】

このうち、STB10a、DVDレコーダ10b、ホームサーバ10cはそれぞれ図1、図2に示した通信過負荷状態回避装置10の構成を備える。

STB10aは、（1）デジタル放送からのストリームデータを受信する処理、（2）ホームサーバ10c又は配信サーバ105等からLAN経由でストリームデータを受信する処理、（3）ストリームデータの再生及びテレビ102への出力処理、（4）ストリームデータをLAN上へ送信する処理などを行う。（1）～（4）は何れもリアルタイム性を要求される処理であるが、このうち（2）と（4）は再送受信により可能な場合もあるので、（1）（3）の方がより厳格にリアルタイム性を要求される。

#### 【0056】

今、STB10aにおいて（1）で受信したストリームデータを（3）で再生出力しているときに、さらに（2）で受信したストリームデータを（3）で再生出力しテレビ102に縮小表示しているものとする。

#### 【0057】

このとき、何らかの原因で（2）の受信データ量が通常よりも大量になり、あるいはSTB10a宛てのフレームが誤って送信されてきて通信過負荷状態になったとする。STB10aは、過負荷状態を検出すると割り込みマスクにより（2）の受信処理を停止により過負荷状態を回避する。これにより、（1）と（3）の処理は、過負荷状態によって再生処理に遅延やフレーム落ちも発生すること

なく、影響を受けず円滑になされる。

#### 【0058】

また、過負荷状態を回避している間に、STB10aは、過負荷状態の終了の検出をしているので、過負荷状態が解消された場合には、元の状態に復旧する。

DVDレコーダ10bは、(a) テレビ放送の受信処理、(b) ホームサーバ10c又は配信サーバ105からLAN経由でストリームデータを受信する処理、(c) ストリームデータの再生及びテレビ102への出力処理、(d) ストリームデータをLAN上へ送信する処理、(e) DVDへの録画処理を主に行う。このうち(a)～(d)は上記(1)～(4)とほぼ同様であるが、DVDレコーダ10bは(e)の録画処理も行う点で処理内容が複雑でかつ処理量が多い。

#### 【0059】

今、STB10aまたは内臓チューナ(図外)からの映像データに対して(e)の録画処理を行うとともに、(b)で受信したストリームデータを(c)で再生出力しているものとする。(e)の録画処理も、(b)から(c)の再生出力処理もリアルタイム性を要求されるが、(e)の録画処理は最も厳格にリアルタイム性が要求される。

#### 【0060】

この場合も通信過負荷状態になったには、上記STB10aと同様に、過負荷状態の検出、回避及び復旧を行う。

ホームサーバ10cは、内臓のハードディスクにストリームデータやファイルなどを記録し、LANを介して他の装置との間でストリームデータやファイルなど送受信する。過負荷状態の検出、回避、復旧についてはSTB10a、DVDレコーダ10bと同様である。

#### 【0061】

このように、STB10a、DVDレコーダ10b、ホームサーバ10cはそれぞれ通信過負荷状態回避装置10を備えることにより、通信の過負荷状態の検出、回避、復旧を行うことができ、しかも、外部の付加装置を必要とせずユーザの判断も必要としないで、装置単体で行うことができる。

#### 【0062】

なお、ネットワーク I/F 104 として用いられるルーターは、通常、ユーザ設定された任意の送信元アドレスやプロトコルを遮断したり、流量制限するフィルター機能を有する場合がある。ところが、このユーザ設定には、煩わしい操作と専門的な知識を必要とする。図 7 の構成では、煩わしいユーザ操作を必要とすることなく、流量制限に相当する過負荷状態の検出、回避、復旧をすることができる。

#### 【0063】

逆に、フィルター機能を使用するようにユーザが設定する場合には、ネットワーク I/F 104 によるフィルター機能と、STB 10a、DVDレコーダ 10b、ホームサーバ 10c の個々の過負荷状態の検出、回避、復旧機能とを組み合わせることによって、機能の分担及び補完を行うことができる。この場合、STB 10a、DVDレコーダ 10b、ホームサーバ 10c 個別に過負荷状態の検出、回避、復旧機能をオン/オフする構成としてもよい。

#### 【0064】

また、図 7 における STB 10a、DVDレコーダ 10b、ホームサーバ 10c の任意の 2 つが組み合わせられて 1 つの装置を構成する場合や、3 つが組み合わせられて 1 つの装置を構成する場合でも、通信過負荷状態回避装置 10 の構成を備えることにより同様の効果を奏することができる。また、パソコン 103 に通信過負荷状態回避装置 10 を備える構成としてもよい。

#### 【0065】

なお、過負荷状態検出部 25 は、データリンク層 (LANチップ 14) に到達した単位時間あたりの受信データ量を測定しているが、ネットワーク層 (IP プロトコル処理部 24) に到達した単位時間あたりの受信データ量を測定して、測定結果をしきい値判定する構成としてもよい。この場合、過負荷状態検出部 25 は、ネットワーク層 (IP プロトコル処理部 24) に到達した単位時間あたりの受信データ量を測定してしきい値判定をする代わりに、ネットワーク層 (IP プロトコル処理部 24) における受信処理がオーバーフローしたか否かを判定するようにしてもよい。

#### 【0066】

また、過負荷状態検出部 25 は、データリンク層（LAN チップ 14）に到達した単位時間あたりの受信データ量を測定しているが、この代わりに、LAN チップ 14 から転送された受信データを一時的に保持するメモリ 12 における受信データ量を測定して、測定結果をしきい値判定する構成としてもよい。

#### 【0067】

なお、上記実施の形態では、過負荷状態検出部 25 は、割り込み信号をマスクすることによりデータリンク層（LAN チップ 14）からネットワーク層（IP プロトコル処理部 24）への受信データの通知を禁止しているが、その代わりに、他の通信階層の間で受信データの通知又は受信データの伝送を禁止する構成としてもよい。例えば、（A）物理層（LAN I/F 15）からデータリンク層への受信データの伝送を禁止してもよいし、（B）物理層、データリンク層、ネットワーク層の何れかの動作をディスエーブルにする構成としてもよい。

#### 【0068】

また、上記実施の形態において、通信過負荷状態回避装置 10 は、通信過負荷状態において、音、光、表示等により通信過負荷状態にある旨をユーザに通知する通知部を備えてもよい。例えば、図 7 に示した STB 10a や DVD レコーダ 10b において、上記の通知部は、通信過負荷状態の検出、回避、復旧のタイミングに合わせてテレビ 102 への映像信号に「通信が過負荷状態になりましたのでしばらくの間受信を制限します」「通信過負荷状態により受信制限中」「通信過負荷状態が解消されました」などの通知を重畳させて、テレビ 102 に表示する構成としてもよい。

#### 【0069】

なお、上記実施の形態において、データリンク層の通信処理はネットワークドライバ 23 と CPU 11 により実現されているが、CPU 11 によらずに専用 LSI チップとして構成してもよい。同様に、ネットワーク層の通信処理（IP プロトコル処理部 24）は CPU 11 によりソフトウェア的に実現されているが、CPU 11 によらずに専用 LSI チップとして構成してもよい。

#### 【0070】

#### 【発明の効果】

以上説明してきたように本発明のネットワーク装置（通信過負荷状態回避装置）によれば、過負荷状態では受信されたデータを無効化するので、ユーザによる判断も付加装置も必要としないで、通信の過負荷状態でも通信処理及び他の処理への影響を除去することができる。つまり、受信処理がCPUの処理能力を占有しないので、その他の処理の品質を落とすことなく継続することが可能となる。それゆえ、一般家庭で使用するネットワーク装置でも容易に適用でき、他の処理を円滑にすることができる。例えば、通信処理以外の他の処理として、リアルタイム性を要求される映像データの処理を行うネットワーク装置であっても通信過負荷状態に起因する影響を排除することができる。

#### 【図面の簡単な説明】

##### 【図 1】

本発明の実施の形態におけるネットワーク装置（通信過負荷状態回避装置）の主要なハードウェア構成を示す図である。

##### 【図 2】

通信過負荷状態回避装置の主要な構成を機能別に表したブロック図である。

##### 【図 3】

過負荷状態検出部における通信過負荷状態検出処理の詳細例を示すフローチャートである。

##### 【図 4】

過負荷状態終了検出部における過負荷状態の終了を検出する処理の詳細例を示すフローチャートである。

##### 【図 5】

実行中のアプリケーション数と、しきい値との対応関係を示す図である。

##### 【図 6】

アプリケーションと、重み付した換算値との対応関係を示す図である。

##### 【図 7】

通信過負荷状態回避装置を適用した家電製品を含むシステム例を示す図である。

##### 【図 8】



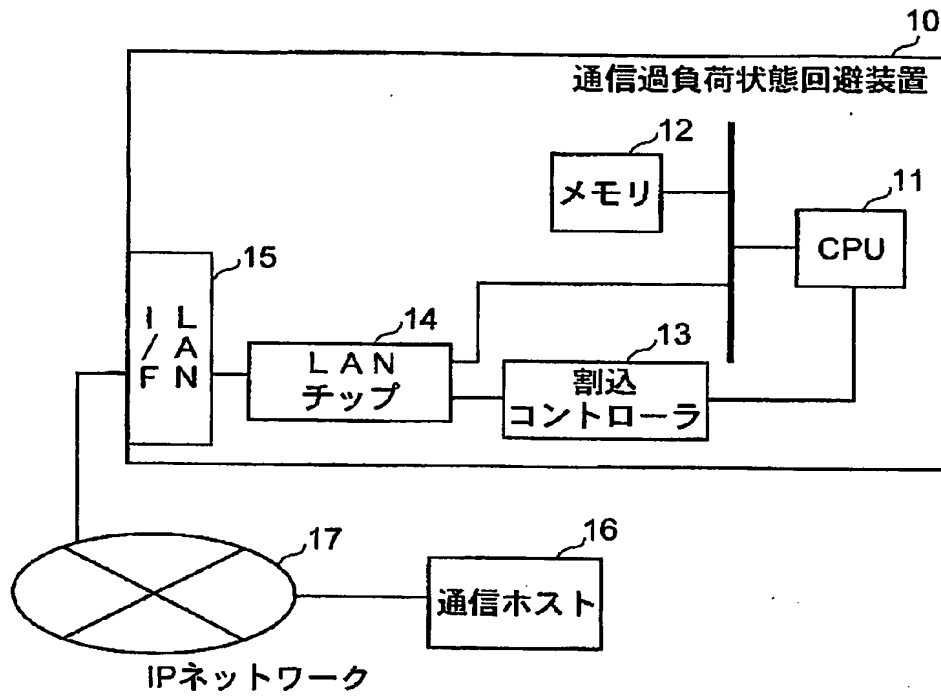
特許文献1に開示された不正アクセス防御システムの構成を示す図である。

【符号の説明】

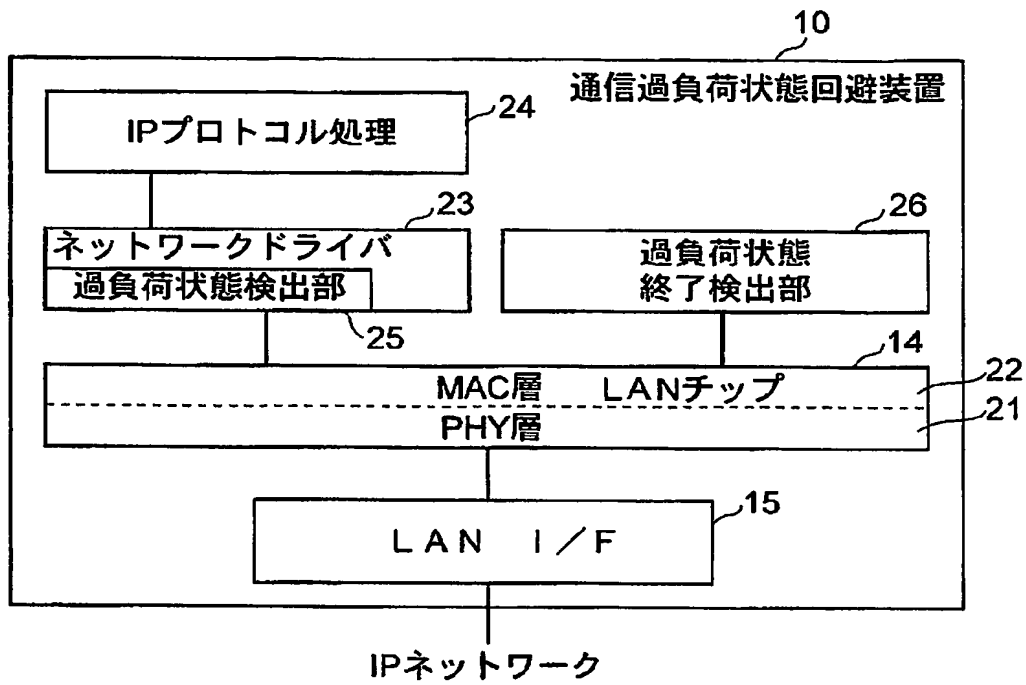
- 10 ネットワーク装置
- 11 CPU
- 12 メモリ
- 13 コントローラ
- 14 LANチップ
- 15 LAN I/F
- 16 通信ホスト
- 17 ネットワーク
- 23 ネットワークドライバ
- 24 IPプロトコル処理部
- 25 過負荷状態検出部
- 26 過負荷状態終了検出部

【書類名】 図面

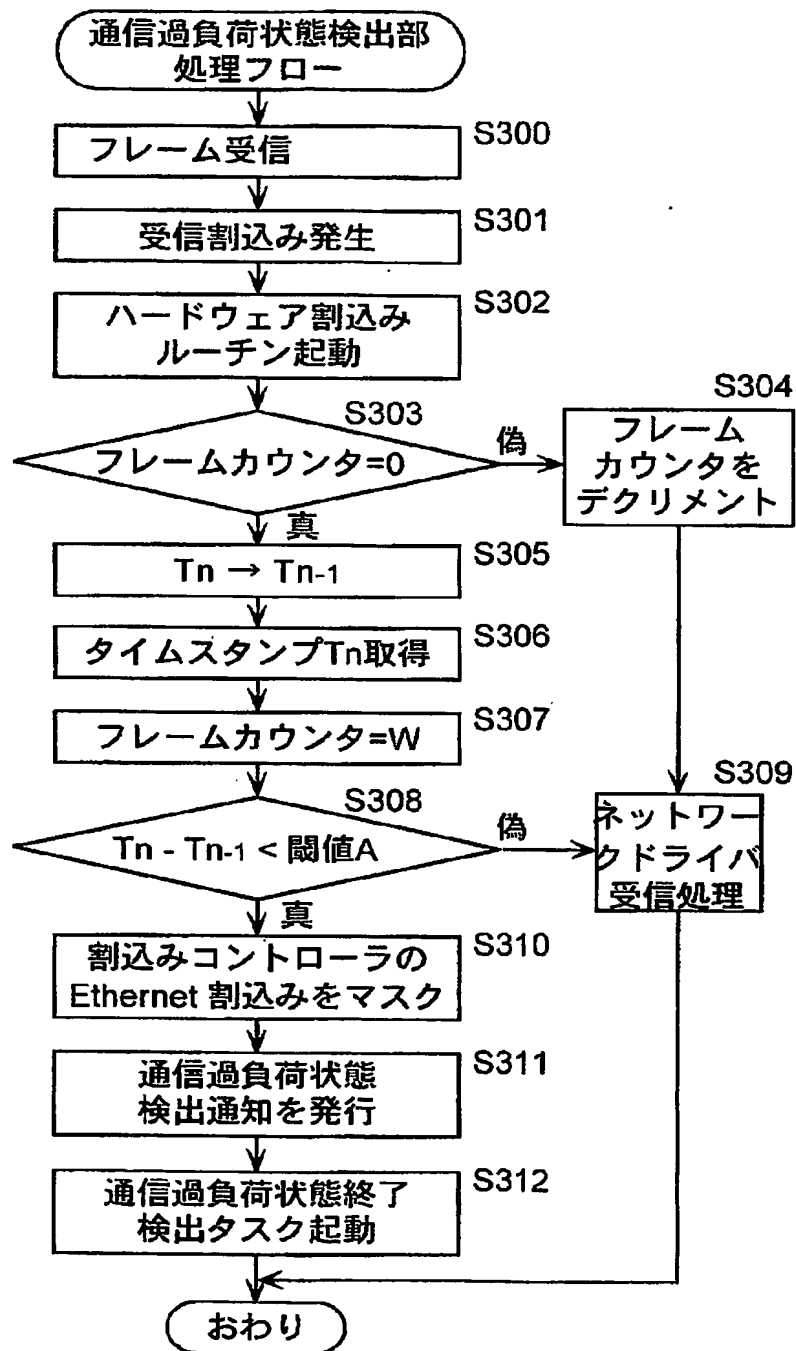
【図 1】



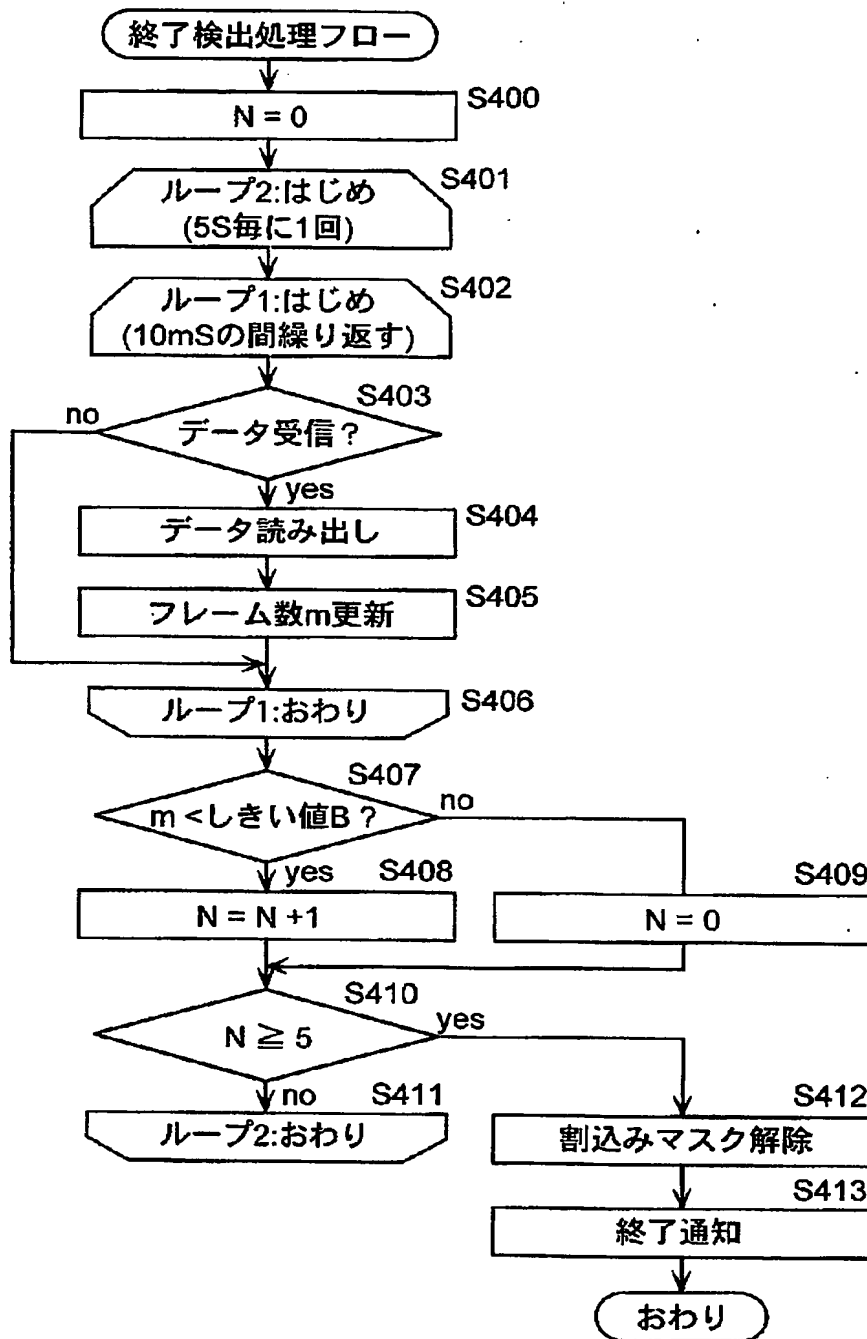
【図 2】



【図 3】



【図4】



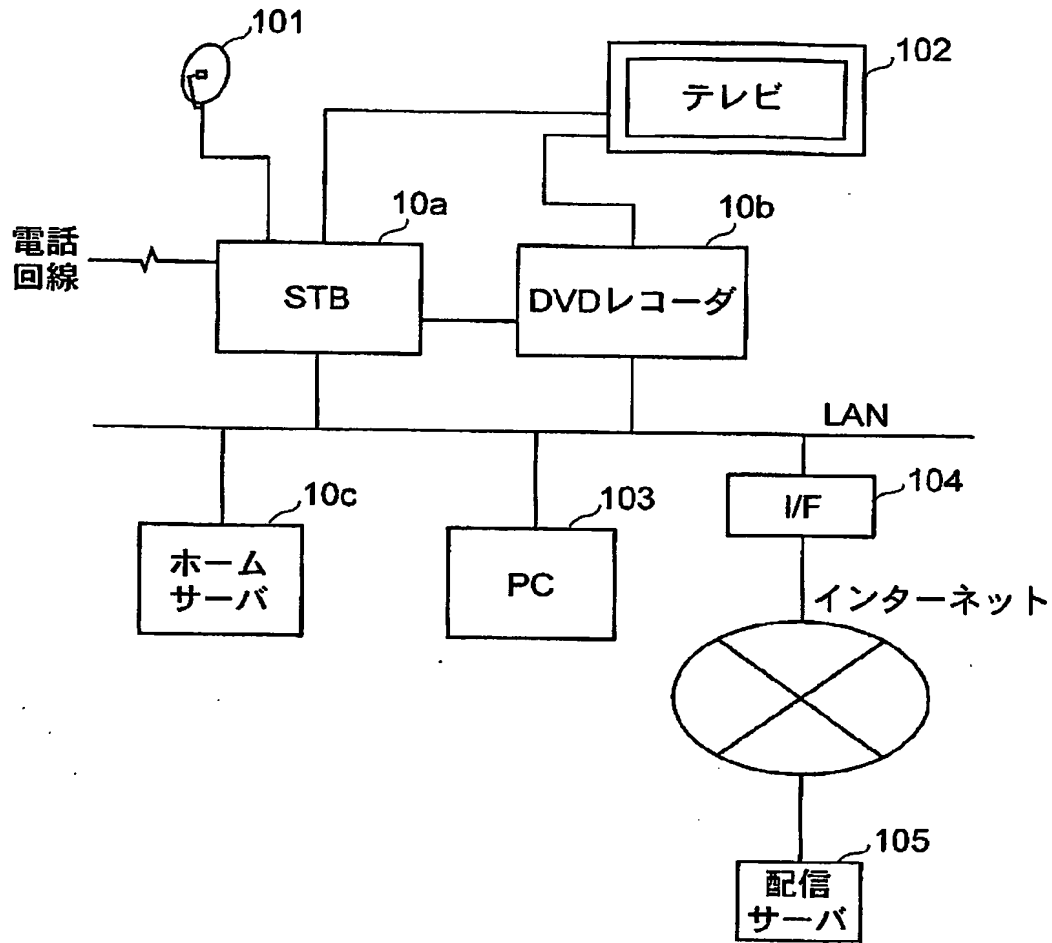
【図5】

アプリケーション数L	しきい値
1	A1
2	A2
3	A3
4	A4
5	A5
6	A6
:	:

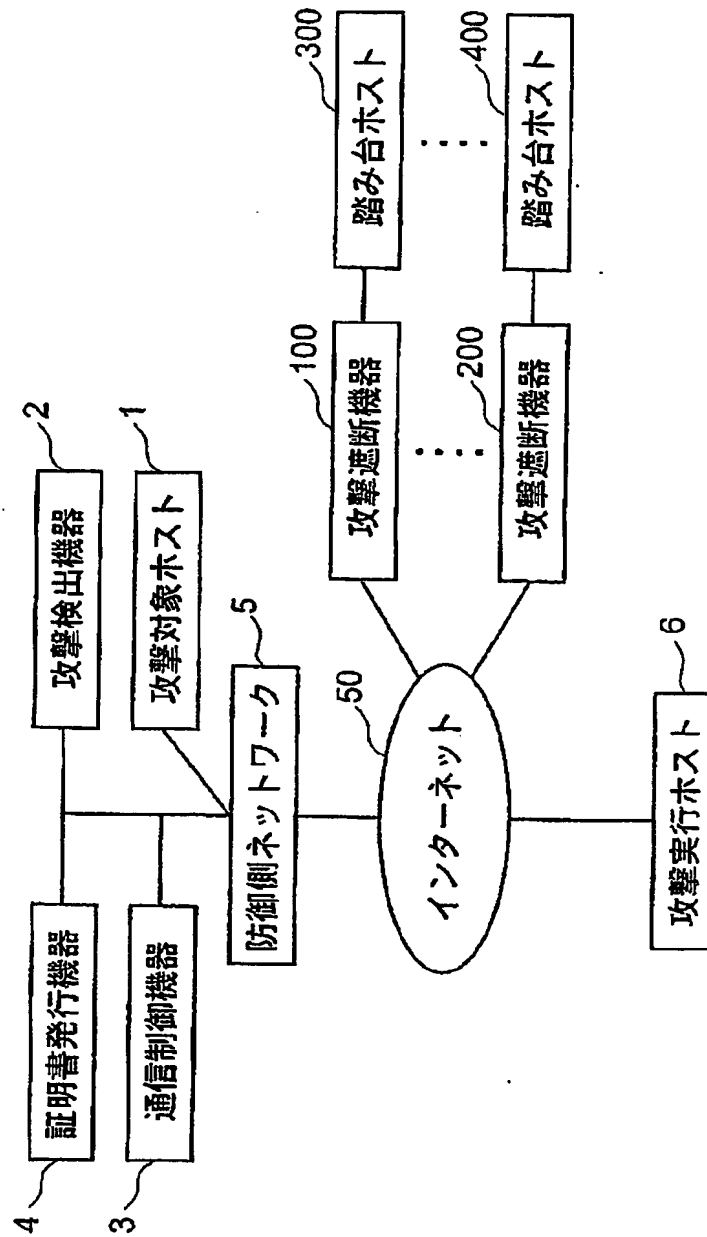
【図6】

アプリケーション名	換算値
App1	1
App2	2
App3	3
App4	1
App5	1
App6	1
:	:

【図 7】



【図 8】





【書類名】 要約書

【要約】

【課題】 ユーザ判断及び外部の付加装置を必要としないで装置単体で通信過負荷状態を回避して、本体の処理を円滑にするネットワーク装置を提供する。

【解決手段】 ネットワーク装置10において、過負荷状態検出部25は、通信が過負荷状態になったことを検出し、過負荷状態を検出したときLANチップ14により受信されたデータを無効し、過負荷状態終了検出部26は、過負荷状態が解消されたことを検出し、解消されたことを検出したとき前記無効化を解除する。

【選択図】 図2

認定・付加情報

特許出願の番号	特願 2002-378555
受付番号	50201980038
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年 1月 6日

<認定情報・付加情報>

【提出日】	平成14年12月26日
-------	-------------

次頁無

特願 2 0 0 2 - 3 7 8 5 5 5

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**